[19]中华人民共和国国家知识产权局

[51]Int.Cl[6]
G06F 13/00
G06F 3/12

[12]发明专利申请公开说明书

[21]申请号 98122672.8

[43]公开日 1999年7月7日

[11]公开号 CN 1221917A

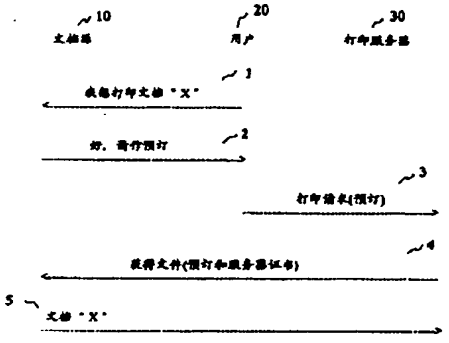
[22]申请日 98.11.23 [21]申请号 98122672.8
[30]优先权
[32]97.11.26 [33]US [31]978793
[71]申请人 国际商业机器公司
地址 美国纽约
[72]发明人 罗格·K·迪布里
[74]专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 于 静

权利要求书5页 说明书14页 附图页数5页

[54]发明名称 授权打印机直接从文件服务器检索文件的系统和方法

[57]摘要

本发明的系统、方法、和程序能使客户系统把从文件源收到的授权传送给打印机，以便直接从文件源检索并打印文件，无需客户系统接收文件的拷贝。客户系统、打印服务器、和文件源通过网络通信连接。当客户系统从文件源请求授权时，文件源生成"预订证书"，该证书包含文件源标识名称、通向文件的路径、文件源的数字签字、有效期、和对于由该文件源生成的证书的唯一的跟踪号码。预订证书发送给客户，客户将其发送给打印服务器。



ISSN1008-4274

权 利 要 求 书

1.用于通过因特网打印驻留在文件服务器的文件的方法，该方法包括以下步骤:

通过第一计算机系统向文件服务器请求授权以便打印文件;

响应该请求从文件服务器向第一计算机系统发出证书以便请求文件，该证书能够传送到打印服务器并包含打印服务器所必须的信息，该信息包括第一计算机系统的因特网地址;

从第一计算机系统向打印服务器发送证书;

从打印服务器向文件服务器发送请求文件并包含作为授权的证书的消息，以便接收文件；以及

在从证书的内容验证了所包含的证书是发给第一计算机系统同一证书之后，从文件服务器向打印服务器发送文件。

2.包括通过因特网通信连接的第一计算机系统、打印服务器、和文件服务器的网络系统，该网络系统包括:

通过第一计算机系统向文件服务器请求授权以便打印文件的装置;

响应该请求由文件服务器向第一计算机系统发出的证书，该证书包含文件服务器的数字签字并包含打印服务器所必须的信息，包括文件服务器的因特网地址，以便请求文件;

用于从第一计算机系统向打印服务器发送证书的装置;

用于从打印服务器向文件服务器发送请求文件的消息的装置，这消息包含作为授权的证书以便接收文件;

用于由文件服务器从证书的内容验证所包含的证书是向第一计算机系统发出的同一证书的装置；以及

用于从文件服务器向打印服务器发送文件的装置。

3.在第一计算机系统中执行的方法，它包括:

通过网络向文件服务器发送请求，以便通过网络以远程打印机打印驻留在文件服务器的文件;

通过网络从文件服务器接收包含文件服务器的数字签字的授权，以便打印文件；以及

通过网络向打印机传送授权，以使打印机随后能够直接从文件服务器取得文件以便打印文件。

4.第一计算机系统包括:

通过网络向文件服务器发送请求的装置，以便通过远程打印机打印驻留在文件服务器的文件;

通过网络从文件服务器收到的包括文件服务器的数字签字的授权，以便通过网络由远程打印机打印文件；以及

通过网络向打印机传送授权的装置，以使打印机随后能够直接从文件服务器取得文件以便打印文件。

5.权利要求 4 的系统，其特征在于，授权包括涉及文件位置的信息。

6.权利要求 4 的系统，其特征在于，授权包括文件服务器的标识名称和文件的路径。

7.在文件服务器中执行的方法，该方法包括:

响应来自第一计算机系统对访问驻留在文件服务器的文件的授权请求，发放其内容包括文件服务器的数字签字的授权证书，该证书能够通过网络从第一计算机系统传送到打印服务器;

通过网络从打印服务器接收请求直接访问供打印的文件的授权证书;

通过证书的内容验证证书是曾发给第一计算机系统而没有改变的同一证书；以及

把文件发送给打印服务器。

8.文件服务器包括:

用于接收来自第一计算机系统的请求授权通过网络由远程打印服务器访问驻留在文件服务器的文件的装置;

响应该请求而生成的计算机可用介质上的数据结构，该数据结构包含打印服务器访问文件所需的信息和文件服务器保证数据结构的有效性所需的信息;

向第一计算机系统发送该数据结构的装置;

用于通过网络从请求直接访问供打印的文件的打印服务器接收数据结构的装置;

用于通过数据结构的内容验证证书为曾发送给第一计算机系统的同一

个而没有改变的数据结构的装置；以及

向打印服务器发送文件。

9.权利要求 8 的文件服务器，其特征在于，数据结构包含文件服务器的数字签字。

10.权利要求 8 的文件服务器，其特征在于，数据结构包含文件服务器的标识名称、通向文件的路径、文件服务器的数字签字、有效期、及由文件服务器生成的数据结构唯一的号码。

11.权利要求 8 的文件服务器，其特征在于，数据结构包括请求中规定的打印机 ID 和打印服务器的网络地址。

12.计算机可用介质上的计算机程序，该程序包括:

用于能够接收来自第一计算机系统的请求授权通过网络由远程打印服务器访问驻留在文件服务器的文件的手段;

响应该请求而生成包含打印服务器访问文件所需的信息和文件服务器保证数据结构的有效性所需的信息的数据结构的手段;

能够向第一计算机系统发送该数据结构的手段;

用于能够通过网络从请求直接访问供打印的文件的打印服务器接收数据结构的手段;

用于通过数据结构的内容验证证书是曾发送给第一计算机系统的同一个而没有改变的数据结构的手段；以及

能够向打印服务器发送文件的手段。

13.在打印服务器中执行的方法，该方法包括:

从第一计算机系统通过网络接收通过网络从文件服务器检索文件的请求，该文件是供打印服务器为第一计算机系统打印的;

接收带有包含打印服务器查找文件和保证从文件服务器检索供打印的文件的授权所需信息的请求的证书;

通过网络向文件服务器发送证书；以及

从文件服务器接收文件。

14.一种打印服务器，它包括:

用于从第一计算机系统通过网络接收通过网络从文件服务器检索文件的请求的装置，该文件是供打印服务器为第一计算机系统打印的;

驻留在计算机可用介质上与请求一同接收的数据结构，该数据结构包含打印服务器查找文件和保证从文件服务器检索供打印的文件的授权所需信息；

通过网络向文件服务器发送该数据结构的装置；以及

用于从文件服务器接收供打印的文件的装置。

15.权利要求 14 的系统，其特征为，保证授权所需的信息是文件服务器的数字签字。

16.通过第一计算机系统、第二计算机系统、和第三计算机系统的网络所执行的方法，该方法包括：

通过第二计算机系统向第一计算机系统请求授权检索文件；

响应该请求，从第一计算机系统向第二计算机系统发出证书，该证书能够被传送到第三计算机系统，并包含第三计算机系统请求文件所需的信息，并能够由第一计算机系统证实；

向第三计算机系统发送该证书并发送从第二计算机系统检索文件的请求；

从第三计算机系统向第一计算机系统发送消息，该消息请求文件、并包含作为检索文件授权的证书；

通过第一计算机系统验证所包含的证书是与曾发给第二计算机系统相同的而没有改变的证书；以及

如果证书被验证有效，则向第三计算机系统发送文件。

17.具有彼此通信链接的第一、第二、和第三计算机系统的网络，用于通过具有打印机的第三计算机系统打印驻留在作为带有文件源的服务器的第一计算机系统的文件，该系统包括：

通过第二计算机系统向第一计算机系统请求授权打印文件的装置；

响应该请求，从第一计算机系统向第二计算机系统发出证书的装置，该证书能够被传送到第三计算机系统，并包含第三计算机系统请求文件所需的信息，并能够由第一计算机系统证实；

向第三计算机系统发送该证书以及发送从第二计算机系统打印文件的请求的装置；

从第三计算机系统向第一计算机系统发送消息的装置，该消息请求文

件、并包含作为检索文件授权的证书；

通过第一计算机系统进行验证的装置，验证所包含的证书是与曾发给第二计算机系统相同而没有改变的证书；以及

如果证书被验证有效，则向第三计算机系统发送文件的装置。

18.权利要求 17 的系统，其特征在于，证书包含文件存储位置的标识名称。

19.权利要求 18 的系统，其特征在于，标识名称包含文件存储位置的因特网地址。

20.权利要求 17 的系统，其特征在于，证书包含通向文件的路径。

21.权利要求 17 的系统，其特征在于，证书包含第一计算机系统的数字签字。

22.权利要求 17 的系统，其特征在于，第三计算机系统是一打印服务器。

23.权利要求 17 的系统，其特征在于，第三计算机系统是一打印系统。

24.权利要求 17 的系统，其特征在于，第三计算机系统是一传真机。

25.权利要求 17 的系统，其特征在于，第一计算机系统包含文件所驻留文件的数据库。

说　明　书

授权打印机直接从文件服务器检索文件的系统和方法

相关申请的交叉对比

本申请涉及共同发明人身份和与其同日提交的序号为 No. 08/979,505 标题为“对打印机或其它网络装置数字证明的安全配置”的共同未决专利申请主题，后者转让给其受让人并在此结合作为对比。

本发明涉及包括但不限于因特网环境的计算机系统的网络，并特别用于安全地打印从网络环境中单独的文件源检索到的文件。

网络环境可能包含无数的配置，包括但不限于使用 TCP/IP 连接、使用令牌环连接等与因特网、广域网、局域网进行通信连接的计算机系统。类似地，计算机系统本身可能从带有最小存储和 CPU 处理功能的网络终端到到个人计算机，包括膝上计算机到工作站以至服务器和大型机变化。计算机之间的关系可能有各种各样，例如彼此相互独立，或具有分布式关系，或具有客户/服务器关系等等。某些或全部文件可能存储在专用的文件存储系统中，例如文件服务器、数据库管理系统等等，或存储在每一系统的存储器内。类似地，打印机可以附加到任何或全部系统上，和/或可能有计算机系统能够与之通信链接的打印服务器。

在网络环境中引起了许多类型的安全性问题。某些文件必须在发送端加密并在接收端解密，以保证在传输期间文件内容不被非授权实体截取。这一安全特性与其它已知的安全特性能够保证文件没有被损坏或保证发送方或接收方的同一性。以下将讨论这其中的某些安全特性。

加密术

以往的密码学，或称传统的对称密码学，用来保护信息内容的保密性。以往的密码学要求加密信息的发送者和接收者共享相同的密钥。同一密钥

即用来对信息扰频(加密)又用来解扰(解密)。 1977 年，国家标准局通过了称为数据加密标准(DES)的块密码算法。与密钥结合使用 DES 算法来保护二进制编码数据。授权用户必须具有曾用来对数据加密的密钥以便对其解密。可能知道 DES 算法但是不知道密钥的加密信息内容的非授权接收者不能对信息内容解密。

这种方法的主要问题是保证发送者和接收者具有密钥，而任何其它人不具有。共享密钥要求一方把密钥发送给另一方。然而，由于许多通信网络是不可靠的，故密钥本身必须加密。如果它以明码发送，就可能有在线路上偷听的人获取密钥并然后能够对双方之间发送的信息进行解密的危险。其它方法是通过挂号邮件发送密钥，但这减慢了通信过程，并如果时间不是重要的问题，何不把信息挂号发送呢。

如上所述，为了防止非授权接收人得到信息内容，密钥必须对非授权用户保密。这样，内容的安全就取决于密钥的安全。于是，必须以安全的方式向授权用户分发密钥。

公开密钥加密术

公开密钥加密术最初由斯坦福大学的 Whitfield Diffie 与 Martin Hellman 于 1976 年提出。它不仅可用来保证传输的信息的保密性，而且能够用于包括数字签字的其它用途。

为了保证传输的信息的保密性，公开密钥加密术解决了以上讨论的安全分发传统加密术中使用的密钥的许多问题。公开密钥加密术基于共同起作用的两种密钥，即私有密钥和公开密钥。个人的公开密钥对其它人是公开的，而它们的私有密钥则是保密的。一个密钥用来加密而另一密钥用来解密信息内容。对于每一加密密钥有一个对应的、但是分开的且不同的解密密钥。以个人的公开密钥加密的信息只能使用该人的私有密钥解密。即使知道了一个密钥而要计算另一密钥也是不可能的。

在公开密钥系统中，不需要传输任何密钥而能够保密地进行通信。例如，每一用户的加密密钥通过分发或公布而公开。任何想要与接收者保密通信的人只要在接收者的公开密钥下加密信息即可。只有拥有保密的解密密钥的接收者才能对传输的信息进行解密。

传统的加密术和公开密钥加密术的结合允许保密密钥保密地发送给有

意向的接收者。发送者使用接收者的公开密钥加密带有保密密钥的信息。然后接收者使用接收者的私有密钥对信息解密并获得用于其它传输的保密密钥。由于公开密钥加密比保密密钥加密慢，故这一方法允许后继传输以便使用较快的传统保密密钥加密术方法。

数字签字

在这些加密系统中，有时仍然需要验证接收信息的发送者实际上是信息中具名的人。基于公开密钥加密术的数字签字用作为证实信息发送者的手段。数字签字允许数字化信息被签字，使得数字化签字的电子信息的任何接收者能够证实信息的发送者，并验证签字信息的完整性。这就是说，保证了接收者接收到的是所发送的信息，而不是伪造的。

为了证实是原始的真正的发送者发送了信息，只需采用判断对方使用了上述的公开密钥加密术对保密通信进行了加密的过程。例如，已经公布了公开密钥的用户在发送信息之前，能够通过使用用户私有密钥对信息加密或使其散列而对信息进行数字化签字。信息的接收者能够通过使用发送者的公共加密密钥对其解密而验证该信息或签字。这一过程刚好与传统加密术相反，即首先由发送者使用发送者私有密钥对信息加密，并由接收者使用发送者的公开密钥进行解密。任何具有发送者公开密钥的人都能够读出信息或签字。保证了任何这种接收者对信息生成者的验证，因为只有具有保密的私有密钥的发送者才能够生成该信息或签字。还对接收者确证了信息没有被掉换，因为这是最初生成的且其上附有数字化签字。任何接收者只需使用签字者的公开密钥就能够证实数字化签字并验证信息的完整性。

在上例中，数字签字是使用发送者私有密钥对信息本身的加密。在数字签字标准(ANSI X9.30 Part I)中，个人的数字签字是附加在任意长的电子信息上的固定长度的位串。为了生成固定长度的数字签字，使用散列函数把任意长度的信息转换为相同固定长度的信息散列或提要。安全散列算法(SHA)是数字签字标准一部分的已知的散列函数。这一信息的散列类似于“手印”，它对于不同的两条信息实际上不能得到相同的散列。在生成信息散列之后，发送者的私有密钥施加到散列以便生成对信息的数字签字。数字签字是被签字的信息和签字者的私有密钥两者的函数。只要私有密钥

保密，数字签字是不能由任何其它人生成的。

在收到数字签字的信息时，接收者使用发送者的公开密钥把数字签字转换为发送者计算的散列。然后，接收者向收到的明语文本信息施加相同的散列函数，并获得收到的信息的散列。如果收到的信息的散列与使用发送者公开密钥转换数字签字所获得的散列相同，则接收者已经证实了发送者的数字签字并验证了签字信息的完整性。

证书

签字者的身份只能保证到使接收者相信公开密钥实际上属于声称是发送者的程度。知道解决这问题的技术的人要依靠某些信托授权，例如政府部门，来保证每一公开密钥与声称是拥有者的人相关联。信托授权将生成称为证书的包含拥有者公开密钥和拥有者姓名的数字信息。授权的表示将以授权本身的数字签字签署数字信息。授权的数字签字将使用授权私有密钥生成，并由接收者使用授权的公开密钥对其辨认，这种公开密钥是广泛传播的并通过电话薄、报纸、和/或因特网 web 网页可获得。这一证书是与发送者信息和发送者的数字签字一同发送的。接收者使用授权的公开密钥解密证书并找到发送者授权的被证明的公开密钥。然后接收者使用发送者被证明的的公开密钥验证发送者签署的信息。这样，能够易于证实证书及验证信息的完整性。

使用证书的访问控制

一般，从另一系统或用户(“用户”)访问计算机系统(“服务器”)的资源是通过口令控制的。这需要服务器维护所有授权用户和每一用户口令的数据库。然而，如果一用户与其它非授权用户共享口令，则降低了口令访问控制系统的完整性。

在基于证书的访问控制系统中，服务器只需要验证证书当局发放的证书。服务器不需要维护关于用户或每一用户对应的口令的数据库。为了获得对服务器资源的访问，用户提交用户的证书。从包含不能被窜改的数据的证书，服务器能够获得用户的授权的公开号码、个人数据、及访问特许权。然后服务器能够向用户传输一随机信息，用户必须使用用户的专用号码对其进行数字签字并返回给服务器。然后服务器能够使用证书中的公开号码验证数字签字，并检验签署的信息与它发送给用户的信息相同。使用

这一数字签字响应，服务器能够确定用户具有对应于证书中授权的公开号码的正确的专用号码。

发送者和接收者之间的安全传输

上述的安全传输技术最好用于信息和/或文件在发送者和接收者之间直接传输的情形。

在任何网络环境中，可能发生用户(通过终端或运行在操作系统上的应用程序与系统个别的交互)需要打印位于距用户遥远的文档的情形。文档可能受到保护防止除了有访问特许权的用户以外的任何人访问。

一般，用户将从远程系统请求文档，远程系统将验证用户具有正确的访问特许权，且如果用户有特许权，则远程系统将向用户发送文档的拷贝。然后用户将向打印机发送文档供打印。然而，这种具有访问特许权的用户可能希望在远程打印机或打印服务器上打印文档，但是不希望在用户自己的本地计算机系统上(为了方便称为客户系统)先检索和存储该文档。由于各种原因，用户可能不希望使文档驻留在用户自己的机器上。例如，某些原因可能多多少少涉及以下方面：客户系统不处于安全的环境中；可能有网络流量上的考虑；或客户系统可能不具有接收文档的存储空间等等。此外，文件服务器可能不希望文件的拷贝存储到客户系统上。文件(例如文档)的拥有者可能希望控制分发的拷贝数量，例如保护文档中的版权或按每拷贝的付费。如果拷贝驻留在客户机上，可能进而从该拷贝作出非法拷贝，或可能对文档作出非法改变。于是，如果打印机能够直接从它可能所存储之处获得文档并打印文档，则可能是更希望的。

然而，为此，如果文档是受到访问保护的，则打印机将需要与用户具有相同的访问特许权。

需要允许打印服务器从原始请求中标识的第三方获得打印文件，使得文档能够通过客户系统原始请求打印文件而没有首先获得文件的情形下被打印。然而，当打印服务器获得文件时，必须向第三方保证请求是有效的(即打印服务器已经被授权获得文件，且原始客户能够合法打印文档)。不知道这种方案在现有的协议下是否可行。

于是本发明的一个目的是在有来自客户的请求时，基于从文件源对客户的授权，允许打印机直接从文件源检索文件。

本发明的另一目的是要提供一种与请求“参照打印”的打印操作的用户有相同访问特许权的打印机。

“参照打印”这一术语在此是用于这样一种打印方案，其中，用户在自己本地计算机上实际上不检索和不存储为了打印而用作为文档的目标拷贝的文档。

本发明的系统、方法和程序能够使用户即客户系统把授权传送给打印机，以便从文件源检索和打印文件。该方案类似于代理为委托人请求事项票据。代理向售票处给出委托人的姓名并收到订票号。代理把订票号给到委托人。然后在事项时间委托人去售票处的“预订售票处”窗口，并向售票处出示订票号和委托人的身份证件(ID)以便收到票。售票处凭他的身份证件，诸如由信托当局即政府发放的驾驶执照，得知委托人是它所声称的那个人；并得知委托人就是要把票给予的人，因为代理在原始请求中对其进行了标识，且委托人出示了与原始请求相同的订票号。

在网络打印环境中，当客户请求打印文件时，文档源(文件源)向客户发出“预订”证书。预订证书保证了对文档访问的授权并能够传送给第三方，即打印机。预订证书是由文件源生成的，并且其内容是基于启动用户对文件源的请求。证书提供了打印服务器请求打印数据所需的信息，诸如文档存储位置的特定名称及通向包含该文档的文件的通路。预订证书还包括文件源验证了由打印机出示给文件源的任何这种预订证书是合法的信息。例如，预订证书包含文件源的数字签字。通过使用关于预订证书其它内容的散列函数，对于该具体的请求(类似于以上类比中订票号的做法)数字签字可以是唯一的签字。数字签字是使用只有文件源知道的私有密钥生成的。预订证书还可能包含用户在其对文件源的原始请求中设定的、作为将要检索和打印文件的打印机的打印机标识 ID 和/或打印机的网络地址。预订证书还可能包含作出原始请求的用户 ID。

客户把预订证书和打印该文件的请求一同发送给打印机。当打印机准备好打印数据时，它向文档源与预订证书一同发送请求该文档的信息。打印机获得文档的授权就是预订证书。由于证书包含了文件源的数字签字，故预订证书不能被窜改。而且，当打印机向文件源出示预订证书时，文件源能够验证，对于包含在预订证书中的文件源的数字签字，打印机就是由

用户起始所标识的打印机，以及打印机处于相同的网络地址。打印机还将向文件源与预订证书一同发送打印机的数字证书，使得文件源能够验证打印机就是所声称的那个打印机。这种数字证书可以是根据共同未决专利申请系列号 No. 08/979,505 配置的数字证书，该专利申请在此结合作为对比。

包含预订证书的其它的实施例可能包括按隐含密钥发送给服务器“购买的”文档。

为了更为完全地理解本发明，现在参照以下在附图中所示的实施例的详细说明，其中：

图 1 表示用户、文档源、及打印服务器之间的信息流，其中“预订”证书包含在某些通信中；

图 2 是表示预订证书结构的框图；

图 3 表示网络配置；

图 4 表示对于使用数字证书控制访问打印系统的用户、打印系统及证书授权当局之间的信息流；

图 5 表示对于使用隐含密码和预订证书的用户、数字库文件源、打印服务器及打印机之间的信息流。

以下将参照表示用户(客户)20 、文档源 10 及打印服务器 30 之间的信息流的图 1 进一步说明本发明的系统、方法和程序。“预订”证书包含在如所示的这些通信之中，并在以下说明。用户(客户)可能是通过网络站、工作站、或运行在任何类型的计算机系统上的应用程序交互的用户。打印服务器可能包括，但是不限于，与网络连接的独立的打印机；或与服务器直接连接的打印机，这里服务器是管理打印机和排队装置的功能的计算机，这或是专门用于这种管理的计算机，或是除了管理之外还执行其它任务的计算机。类似地，文件源可能是一计算机系统，这可能是也可能不是专门管理系统的存储装置上的文件的计算机。这类文件服务器可能包括，但是不限于，数据库管理系统或数字化库等。

本发明的系统、方法和程序向用户 20 提供了通过通信 1 访问文档源 10 并请求希望打印文档的能力。应当注意，本发明对于用户可能必须付费的情形允许获得将其打印的权力，和/或提供一口令以获得对它的访问。这些情形在以下其它实施例中讨论。

在收到打印文档的请求时，文档源 10，或文档的拥有者，将基于该特定用户的请求生成预订证书，并将通过通信 2 向请求的用户给出证书。

预订证书 40(图 2)包含以下字段：文档源的识别的名称 41，该名称告知打印服务器确切地在那里可以获得该文档(例如包含因特网地址)；通向文档文件的路径 42，以便在文件系统内找到该文档；以及文档的提供者的数字签字 43。当文档源生成了预订证书时，文档源使用其自身的私有密钥数字签署预订证书。预订证书还包含指示证书有效截止期的日期 44，以及为跟踪记录之用的序列号 45。序列号是由文件源发出的对每一预订证书唯一的。这一唯一的序列号还能够由文件源以类似于当基于“预订”请求票据时给出的顺序号的方式作跟踪之用。

预订证书还可能包含含有请求打印文件的用户的用户 ID，及将由用户用来检索和打印文件的打印机 ID 及打印机的网络地址的字段。预订证书还可能包含口令或其它保密信息或密钥。

反过来参见图 1，用户 20 取出“预订”证书，建立打印请求，并向打印服务器通过通信 3 发送打印请求。打印请求规定了所要请求的哪一个文档，以及文档在哪里。请求还包含“预订”证书，该证书向打印机给出访问文档源以获得文档的凭证。

打印服务器 30 通过通信 4 访问文档源 10，请求文档，并向文档源给出证实打印机被允许获得该文档的预订证书。打印服务器还向文档源给出服务器证书或数字证书。一种用于本发明优选实施例的这样的数字证书在共同未决的申请书中公开，其序号为 No. 08/979,505，标题为“打印机或其它网络装置数字证书的安全配置”，该申请与此同日提交并在此结合对照。这一数字证书向文档源证实了该打印服务器即是打印服务器本身表示的那个打印服务器。

如果本发明的实施例在预订证书中包含了由作出请求的用户对预订证书规定的打印机 ID 和打印机网络地址的字段，则文档源还能够证实请求文件的打印机就是由用户对文档源规定的同一打印机。文档源还能够验证打印请求来源于由用户规定的并记录在预订证书中的同一网络地址。

当文档源 10 收到预订证书时，文档源验证这一证书的确就是由文档源原本发出的的那个证书。文档源知道数字签字是只有文档源才能使用其私

有密钥产生的那个数字签字。如果数字签字是唯一的，即它是基于预订证书的内容通过使用关于内容的散列函数的，那么文档源就能够使用其私有密钥把数字签字解密为散列值。然后文档源能够把相同的散列函数施加到收到的预订证书的内容上，并比较所得的散列，以证实在文档源签置了预订证书之后预订证书中没有数据发生变化(例如文件的名称，打印机 ID 等)。在其它实施例中，特别是没有唯一数字签字的那些实施例中，文档源能够对每一由相关标识信息(诸如要检索的文件名称和由请求用户原本规定的打印机的 ID 等)发出的预订证书，使用对于该预订证书唯一的序列号，保持其自身的登录或数据库。然后，当预订证书回收时，文档源能够参照预订证书中的序号，并确定发出的预订证书中的信息是否与收到的预订证书中的信息匹配。

在证实了打印机就是所声称的打印机，并验证了预订证书对由文档源发出的预订证书没有改变之后，文档源能够安全地通过通信 5 向打印机发送文档。

网络实施例

本发明的另一实施例示于图 3，其中打印服务器 30 处于物理上安全的环境 A，使得对打印机输出的物理访问由“锁和密钥”或通过包括口令启动机制、标记锁等其它类似的控制访问手段限制。文件源服务器 10 和用户/客户 20 可能处于也可能不处于同一物理环境，或它们可能完全不在一个物理安全的环境之中。类似地，打印机、客户、和服务器可能与诸如因特网等通信链路 50 不安全的网络进行通信链接。

使用上述的本发明，用户 20 从服务器 10 对特定的文件请求预订证书。用户 20 借助该请求向服务器 10 发送来自信用当局的用户的数字证书。服务器 10 能够或者拥有访问控制名单的数据库，以确定请求的用户是否有权访问所请求的文件，或者访问授权可能是用户的数字证书的一部分。一旦服务器 10 确定了用户 20 被授权访问文件，则如上所述服务器 10 发送预订证书，该预订证书是使用服务器 10 在用户的数字证书中收到的用户的公开密钥而加密的。用户使用用户私有密钥解密预订证书，并使用下述用户从打印机的数字证书收到的打印机的公开密钥对其进行加密。然后用户 20 能够向打印机服务器 30 与加密的预订证书一同发送打印请求，预订证书包含

服务器的辨识名称，到达请求的文件的路径，以及使用服务器私有密钥加密的服务器的数字签字。当打印系统收到加密的预订证书时，打印机将使用打印系统的私有密钥对其进行解密。

图 4 示出数字证书如何能够用来控制对打印系统 30 的访问。打印机 30 可能具有某种类型的访问控制名单，或访问授权可能在从潜在的用户 20 收到的数字证书中规定。证实请求访问的用户就是所声称的用户，这可能是必要的。除了防止其安全性质不清的用户使用打印机之外，其它非授权用户还可能绕过简单的识别/口令模式来破坏打印机中的密钥配置信息，包括闪速存储器中的信息。

请求访问的用户将向打印机与包含用户公开密钥的用户数字证书一同发送这种请求 401 。然后打印机可向验证当局 60 发送这公开密钥和用户标识 402 以便证实用户的数字证书。现在打印系统具有用户的公开密钥并知道其是经过证实的。打印机向用户发送随机信息 403 。用户以其私有密钥加密该信息并向打印机发送回该信息 404 。打印系统使用用户的公开密钥解密信息。如果它与原来的信息匹配，则打印系统得知用户就是所声称的那个用户。

现在能够对照管理上所建立的访问控制名单(ACL)验证访问特许权。如果在 ACL 中得到证实，则只需允许进一步的操作。例如，只有授权的管理员能够建立安全邮箱，重新配置打印机，加载新的数字证书等。操作者能够取消工作事项，但是最终用户只能提交打印工作作业。类似地，图 3 中用户 20 的打印授权将如此被验证。

反过来参见图 3 ，现在既然打印机已经验证用户 20 的真实性和授权，则打印机向服务器连同现已使用打印机私有密钥加密的预订证书一同发送文件请求。打印机还发送打印机的数字证书。打印机的数字证书能够通过在共同未决的申请书中所述的过程生成，该专利申请书序号为 No. 08/979,505 ，标题为“打印机或其它网络装置数字证书的安全配置”，该申请在此结合对照。

基本上，打印机的数字证书是通过使打印机制造商在制造过程中把密钥置入打印机内部的过程而生成的。打印机序列号、打印机型号、和密钥记录在由诸如打印机制造商等验证当局维护的安全数据库中。当请求数字

证书时，打印服务器向验证当局发送两部分的信息。第一部分包括打印机序列号和型号，第二部分包括这一相同的信息但是使用了打印机内置的密钥加密。验证当局在安全数据库中查找型号和序列号并找到密钥。密钥是用来对信息的第二部分解密的。如果信息的第二部分解密的部分与第一部分匹配，则打印机已经得到验证。然后当局向打印机发送以密钥加密的数字证书。授权包括给予打印机的证书中的公开密钥并把对应的私有密钥以来自数据库的密钥编码。编码的密钥与数字证书一同发送到打印机。在一个实施例中，应当注意，置入打印机和当局的数据库中存储的密钥只能在打印机和当局之间使用用于产生数字证书。在这种实施例中，密钥不能用于任何使用传统的对称加密术的其它通信。但是其它的实施例可能确实使用了置入的密钥用于其它的这种通信，当然是认识到验证过程可以有某些折中方式。

然后文件服务器10使用从打印机的数字证书中找到的公开密钥并对带有文件请求的预订证书解密。

应当注意，打印机还能够产生第二密钥，使用其私有密钥对其加密，并把它发送到服务器。然后服务器将使用来自打印机的数字证书的公开密钥对该密钥进行解密。在另一实施例中，服务器能够产生一个密钥并把使用打印机的公开密钥加密的这一密钥发送到打印机。服务器能够使用该密钥或者打印机公开密钥加密该文件。文件服务器把加密的文件发送给打印机。打印机使用适当的密钥解密文件。因为公开密钥加密比保密密钥加密慢，故一个实施例使用这一方法。因而，对于由打印机进行解密的大的文档，服务器将使用保密密钥加密。然后打印机能够使用相同保密密钥对文件进行解密。

隐含密码(Cryptolope)实施例

以下说明隐含密码及预订证书的一种可能的应用，以便在电子商务环境中提供文档的安全打印。假设在正在全球出现的电子商务中，出版者常常要销售一次性打印拷贝权，这正象他们销售一本打印的书或杂志那样。允许可打印版本出现在系统内任何明显之处将把出版者置于危险的境地，因为可能作出非法拷贝和打印多次。即使加密的文档在其到打印机的途中要被假脱机并解密，也可能通过以软件代替实际的打印机而哄骗系统。因

而，在这种环境中的打印机这样才是安全的，即允许它们证实自己，提供唯一的公开加密密钥，并使用标准的解密算法解密并打印传送的(on the fly)文档。

如图5所示，最终用户20确定用户想要购买文档的可打印拷贝，501。这版本可能在格式编排、高质量图象和字模的使用上不同于非打印版本。它可能加水印以保护版权。作为购买交易的一部分，最终用户被告知，最终用户必须访问经过验证的、安全的打印机获得这一文档，并必须提供打印机的公开密钥证书，502。然后用户使用SNMP get从打印机获得证书，503。假设打印机公开密钥证书存储在打印机中的SNMP MIB中，504。如前所述，打印机公开密钥证书与验证打印机必要的信息一同包含有打印机公开加密密钥。这是重要的一个步骤，因为出版者必须确信打印机是用户所声称的那个打印机。该证书发送给出版者，505 - 507。

出版者向用户发送预订证书，508。用户向打印服务器发送预订证书和出版者的URL，509。打印服务器向出版者/服务器发送“获得打印文件”的消息515，并包括预订证书和打印机证书。

现在出版者为文档建立隐含密码并把它发送给用户。文档本身以对称密钥加密，且使用打印机的公开密钥对该密钥加密，520。

隐含加密的文档发送给打印服务器被打印。打印服务器把加密的文档置于假脱机，525，并保持加密密钥直到打印机请求该密钥。

打印机请求一个新的打印作业，且加密的文档发送到打印机530。打印机理解，这是加密的文档，并从打印服务器请求密钥，535。服务器发送密钥，540，该密钥本身是使用打印机公开密钥加密的。打印机解密该密钥，并然后在它打印文档时使用该密钥解密文档。

使用上述说明书，通过使用标准的编程和/或工程技术生产编程软件、固件、硬件，或它们的任何组合，本发明可以作为机器、过程、或制成品实现。

任何所得到的具有计算机可读程序代码的程序，在诸如存储器装置或传输装置等一个或多个计算机可用介质内可以实施，从而制成根据本发明的计算机程序产品或制成品。至于这里所使用的“制成品”及“计算机程序产品”这些术语，是指形成在任何计算机可用介质，诸如任何存储器装

置或在任何传输装置中(永久地、暂时地、或瞬间地)存在的计算机程序。

直接从一种介质执行程序代码，把程序代码存储到介质，从一种介质向另一种介质复制代码，使用传输装置传输代码，或其它相当的行为可能涉及只是暂时作为在制造、使用或出售本发明中最初或最后步骤实施程序代码的存储器或传输装置的使用。

存储器包括，但不限于，固定(硬)盘驱动器、软盘、光盘、磁带、半导体存储器，诸如 RAM 、 ROM 、 Porms 等。传输装置包括，但不限于，因特网、内连网、电子公告牌和消息/通知交换、基于电话/调制解调器的网络通信、硬导线/电缆通信网络、蜂窝式通信、无线电波通信、卫星通信、及其它固定或移动通信网络系统/通信链路。

实施本发明的机器可能涉及一个或多个处理系统，这包括，但不限于，CPU 、存储器/存储装置、通信链路、通信/传输装置、服务器、 I/O 装置、打印机、或实施如同权利要求所述的本发明的一个或多个处理系统的任何部分组件或个别部件，包括软件、固件、硬件、或它们的任何组合或部分组合。

计算机科学业内专业人员将能够易于组合所述生成的软件与适当通用或专用计算机硬件而生成实施本发明的计算机系统和/或打印系统和/或部分组件，并生成用于执行本发明的方法的计算机系统和/或打印系统和/或部分组件。

虽然已经详细解释了本发明的优选实施例，但是对于业内专业人员来说很明显，在不背离以下权利要求中所述的本发明的精神和范围的情形下，可以出现对实施例的变形和修改。例如某些变形和修改包括如下情形:

所述实施例可以具有另外的不是以上具体所述的安全交易特点，或者上述的特点或特点的各种组合可以从其它实施例中省略。

还应当注意，“文件”和“文档”这些术语在这里交替使用，其用意是任何文档也是文件，虽然文件可能不一定限于文档。即使当使用“文档”这一术语时，是指其更为广泛的“文件”含义，因为术语“文档”在这里只是用作为文件的例子。

而且，术语打印机、打印服务器、和打印系统在这里交替使用。其中打印机的功能描述为或是指，假设打印机已经把它和必要的功能联系在一

起而能执行诸如连接到计算机上的独立打印机的那些功能，即是一个打印系统，或打印服务器或打印机控制器等等．此外，传真机在本发明的上下文中也可理解为打印机。

而且，术语文件服务器、文件源等等在这里不严格而交替使用。任何这种术语是指控制驻留文件存储器的任何计算机系统．服务器不一定是指客户/服务器技术意义中专用的服务器，虽然它可以是这样的服务器。类似地，在这里不严格地使用的术语“客户”是指请求者，而并不一定指客户/服务器环境中任何客户的典型的具体硬件或软件配置，虽然并不排除这种含义。

说 明 书 附 图

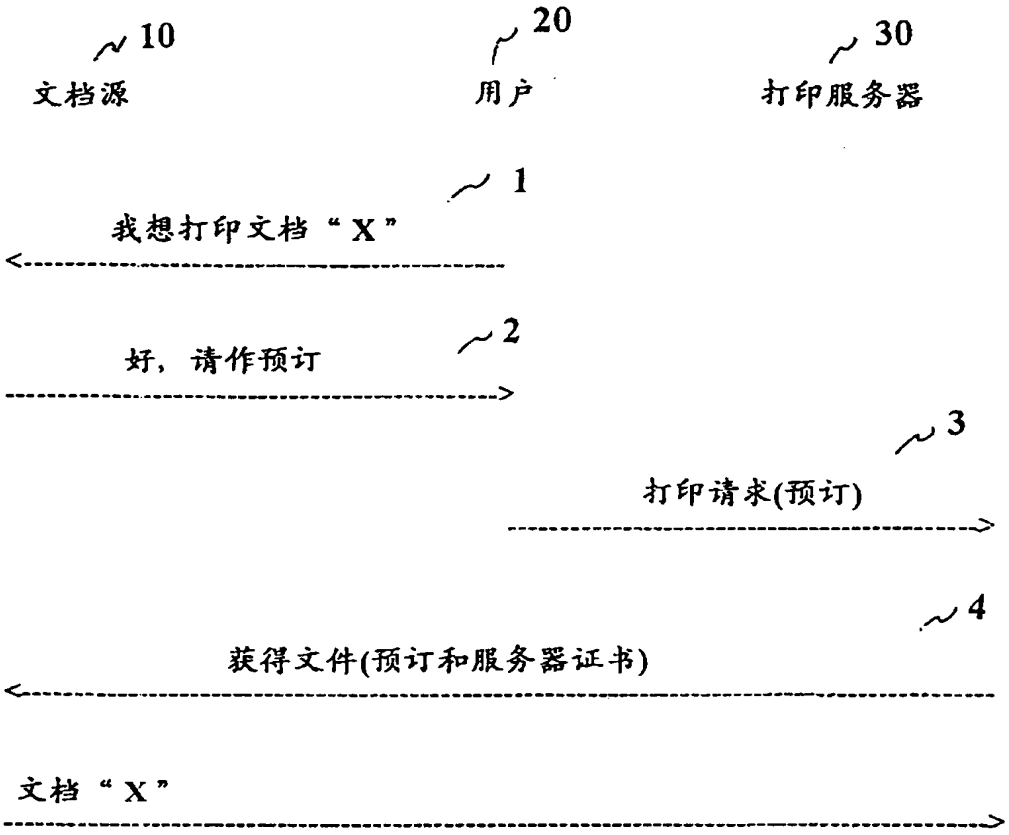

10
文档源
20
用户
30
打印服务器
1
我想打印文档“X”
2
好，请作预订
3
打印请求(预订)
4
获得文件(预订和服务器证书)
5
文档“X”

图 1

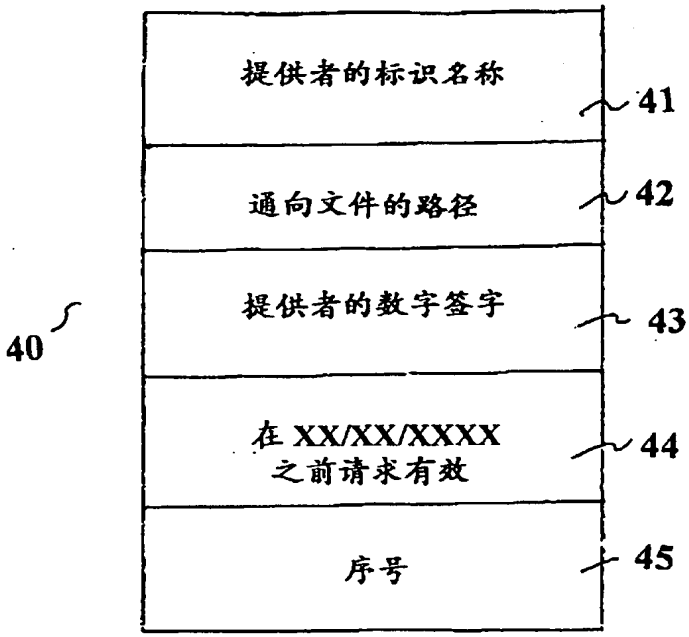


图 2

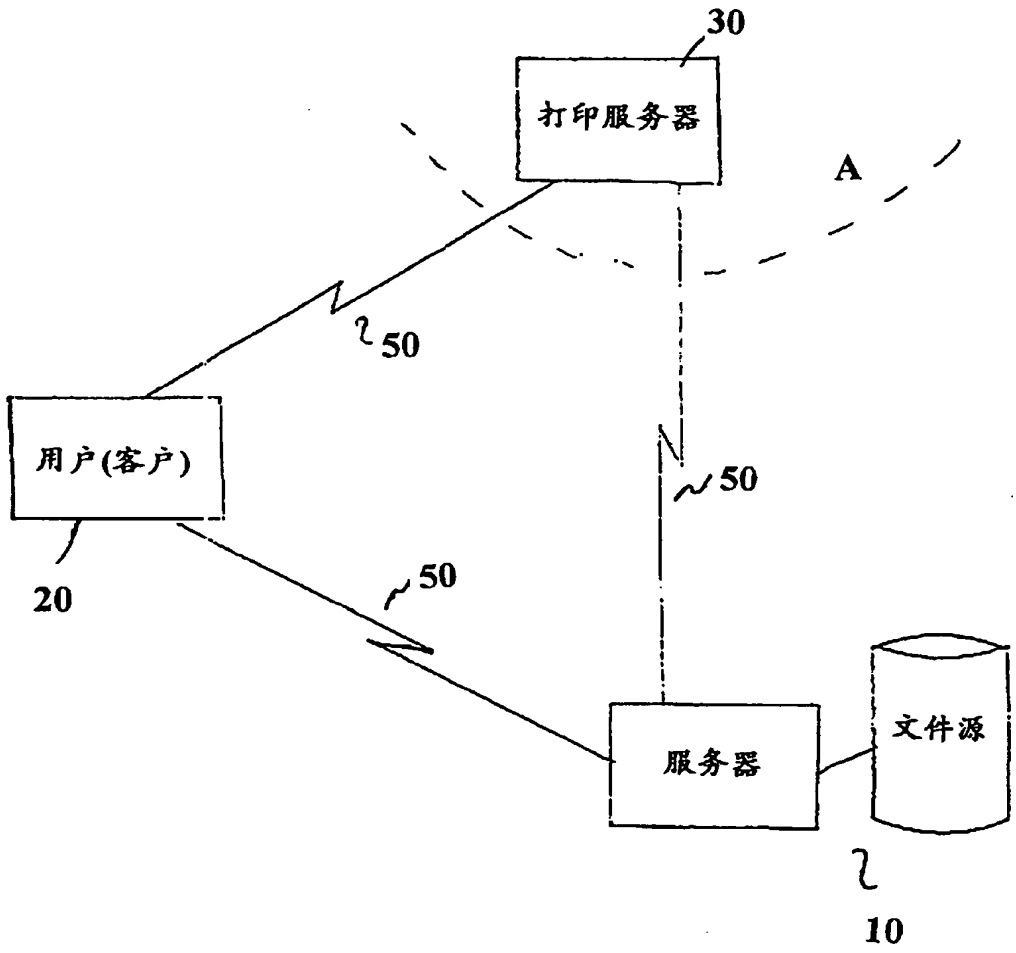


图 3

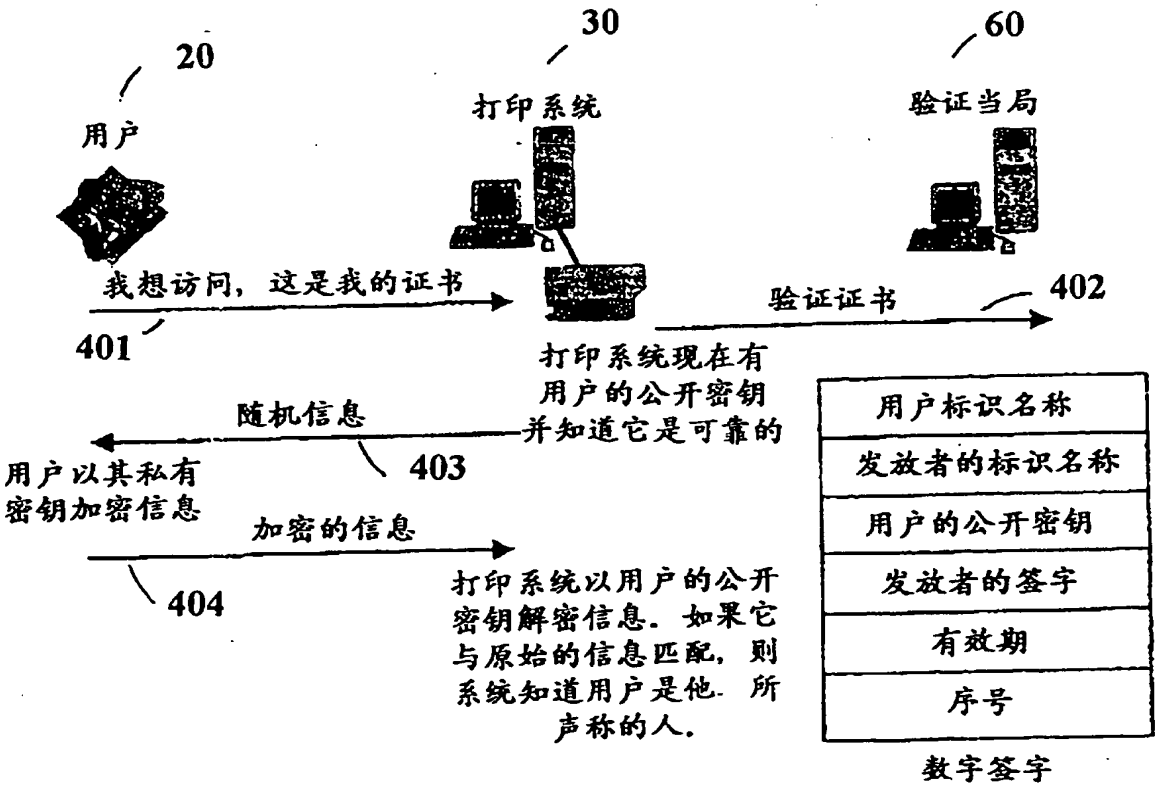
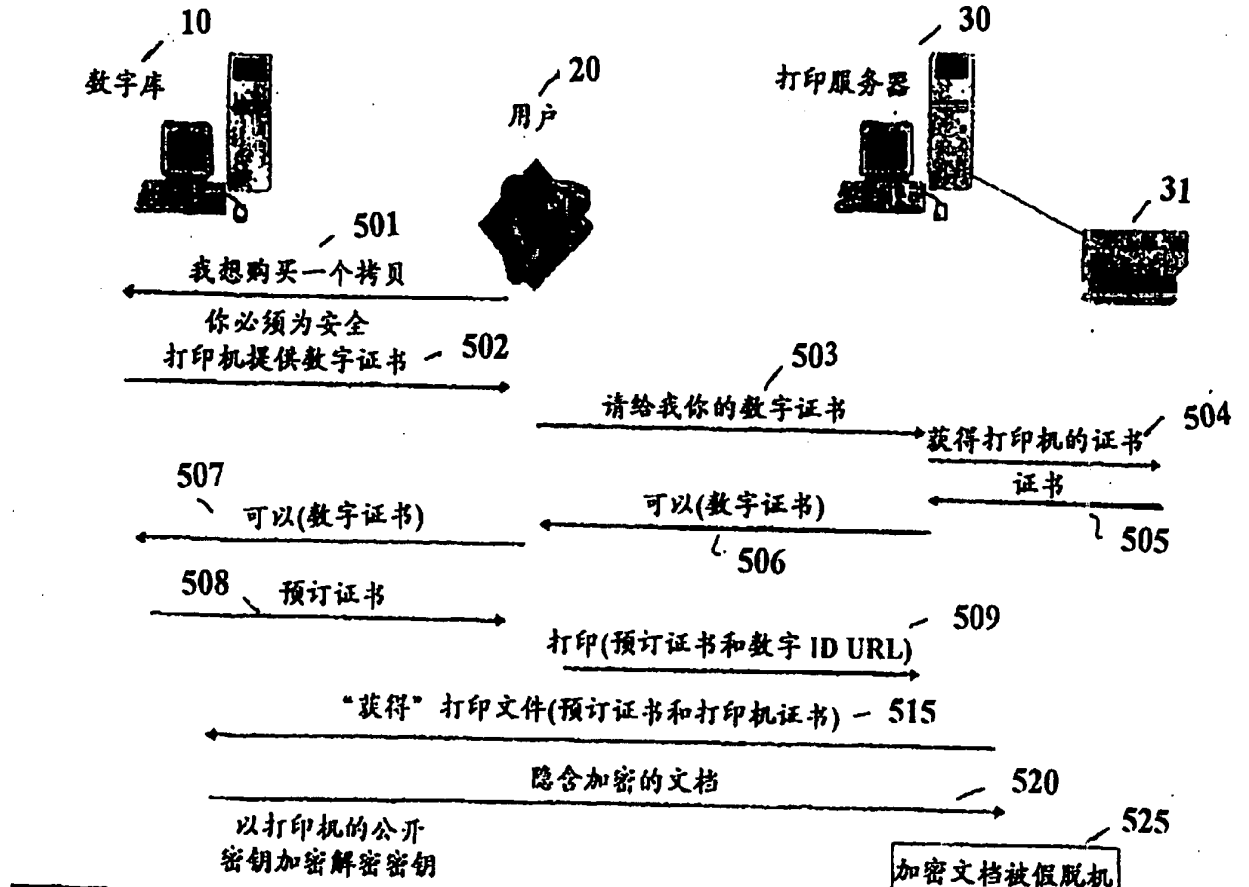

20
用户
30
打印系统
60
验证当局
我想访问，这是我的证书
401
验证证书
402
打印系统现在有
用户的公开密钥
并知道它是可靠的
随机信息
403
用户以其私有
密钥加密信息
加密的信息
404
打印系统以用户的公开
密钥解密信息。如果它
与原始的信息匹配，则
系统知道用户是他所
声称的人。
用户标识名称
发放者的标识名称
用户的公开密钥
发放者的签字
有效期
序号
数字签字

图 4



文档源的标识名称
通向打印文件的路径
文件源的数字签字
在 XX/XX/XXXX 之前请求有效
序号

预订证书

图 5